A PROBABILISTIC TITS ALTERNATIVE AND PROBABILISTIC IDENTITIES

MICHAEL LARSEN AND ANER SHALEV

ABSTRACT. We introduce the notion of a probabilistic identity of a residually finite group Γ. By this we mean a non-trivial word w such that the probabilities that $w = 1$ in the finite quotients of Γ are bounded away from zero.

We prove that a finitely generated linear group satisfies a probabilistic identity if and only if it is virtually solvable.

A main application of this result is a probabilistic variant of the Tits alternative: let Γ be a finitely generated linear group over any field and let G be its profinite completion. Then either Γ is virtually solvable, or, for any $n \geq 1$, n random elements $g_1, \ldots, g_n$ of G freely generate a free (abstract) subgroup of G with probability 1.

We also discuss related problems and applications.

1. Introduction

The celebrated Tits alternative [Ti] asserts that a finitely generated linear group is either virtually solvable or has a (nonabelian) free subgroup. A number of variations and extensions of this result have been obtained over the years. In particular it is shown by Breuillard and Gelander [BG] that if Γ is a finitely generated linear group which is not virtually solvable then its profinite completion $\widehat{\Gamma}$ has a dense free subgroup of finite rank (this answers a question from [DPPS], where a somewhat weaker result was obtained). The purpose of this paper is to establish a probabilistic version of the Tits alternative, and to relate it to the notion of probabilistic identities, which is interesting in its own right.

In order to formulate our first result, let us say that a profinite group G is *randomly free* if for any positive integer n the set of n-tuples in G^n which freely generate a free subgroup of G (isomorphic to F_n) has measure 1 (with respect to the normalized Haar measure on G^n). We also say that a (discrete) residually finite group Γ is randomly free if its profinite completion is randomly free.

Recall that related notions have already been studied in various contexts. For example, in [Ep] it is shown that connected finite-dimensional nonsolvable real Lie groups are randomly free (in the sense that the set of n-tuples which do not freely generate a free subgroup has measure zero). We can now state our probabilistic Tits alternative.

Theorem 1. *Let Γ be a finitely generated linear group over any field. Then either Γ is virtually solvable or Γ is randomly free.*

The proof of this result relies on the notion and properties of probabilistic identities which we introduce below.

Let $w = w(x_1, \ldots, x_n)$ be a non-trivial element of the free group F_n, and let Γ be a residually finite group. Consider the induced word map $w_\Gamma : \Gamma^n \to \Gamma$. If the image (denoted by $w(\Gamma)$) of this map is $\{1\}$ then w is an *identity* of Γ. We say that w is a *probabilistic identity* of Γ if there exists $\epsilon > 0$ such that for each finite quotient Γ/Δ of Γ, the probability $P_{\Gamma/\Delta}(w)$ that $w(h_1, \ldots, h_n) = 1$ (where the $h_i \in \Gamma/\Delta$ are chosen independently with respect to the uniform distribution on Γ/Δ) is at least ϵ. This amounts to saying that, in the profinite completion $\widehat{\Gamma}$ of Γ, the probability (with respect to the Haar measure) that $w(g_1, \ldots, g_n) = 1$ is positive.

For example, $w = x_1^2$ is a probabilistic identity of the infinite dihedral group $\Gamma = D_\infty$, since in any finite quotient $\Gamma/\Delta = D_n$ of Γ we have $P_{\Gamma/\Delta}(w) \geq 1/2$.

More generally, probabilistic identities may be regarded as an extension of the notion of coset identities. Recall that a word $1 \neq w \in F_n$ is said to be a *coset identity* of the infinite group Γ if there exists a finite index subgroup $\Delta \subseteq \Gamma$ and cosets $g_1\Delta, \ldots, g_n\Delta$ (where $g_i \in \Gamma$) such that $w(g_1\Delta, \ldots, g_n\Delta) = \{1\}$.

Our main result on probabilistic identities is the following.

Theorem 2. *Let Γ be a finitely generated linear group over any field. Then Γ satisfies a probabilistic identity if and only if Γ is virtually solvable.*

Theorem 2 has several consequences.

First, it implies that a finitely generated linear group which satisfies a coset identity is virtually solvable, a result which was proved in [BG] (see Theorem 8.4 there) using other tools.

Secondly, Theorem 2 easily implies Theorem 1. To show this, suppose Γ is not virtually solvable, and let G be the profinite completion of Γ. Note that $g_1, \ldots, g_n \in G$ freely generate a free subgroup of G if and only if $w(g_1, \ldots, g_n) \neq 1$ for every $1 \neq w \in F_n$. By Theorem 2 above, the probability that $w(g_1, \ldots, g_n) = 1$ is 0 for any such w. As Haar measure is σ-additive, the probability that there exists $w \neq 1$ such that $w(g_1, \ldots, g_n) = 1$ is also 0. Thus, $g_1, \ldots, g_n$ freely generate a free subgroup with probability 1, proving Theorem 1.

Next, Theorem 2 immediately implies the following.

Corollary 3. *A finitely generated linear group which satisfies a probabilistic identity satisfies an identity.*

It would be interesting to find out whether the same holds without the linearity assumption. We discuss this and related problems and applications in Section 3 below.

Our original approach to proving Theorem 2 relied on strong approximation for linear groups and on establishing upper bounds on the probabilities $P_G(w)$ where G is a group satisfying $T^k \leq G \leq \mathrm{Aut}\,(T^k)$ for a finite simple group T. However, this approach is rather long and depends on the classification of finite simple groups. A shorter and classification-free proof of Theorem 2 is given in Section 2 below.

The idea is to use linearity to map Γ into a linear algebraic group G over an infinite product $\prod_{\mathfrak{m}} A/\mathfrak{m}$ of finite fields. The closure of the image is then a profinite group. Suppose that for some Zariski-closed subset $X \subset G^n$, the measure of the closure of $X(\prod_{\mathfrak{m}} A/\mathfrak{m}) \cap \Gamma^n$ is positive. Unless X is a union of connected components of G^n, by intersecting X with a suitable translate by an element of Γ^n, we find a smaller closed subset with the same property. This process cannot

continue indefinitely. The theorem is obtained by applying this to any fiber of a non-trivial word map w. The actual implementation uses the language of (affine) schemes.

In fact this method of proof yields the following extension of Theorem 2: *Suppose Γ is a finitely generated linear group which is not virtually solvable. Then all fibers in $(\widehat{\Gamma})^n$ of all non-trivial words $w \in F_n$ have measure 0.*

In other words, for a finite group G, let $P_{G,w}$ denote the probability distribution induced on G by w (so that, for $g \in G$, $P_{w,G}(g)$ is the probability that $w(g_1, \ldots, g_n) = g$). Its ℓ_∞-norm is defined by $||P_{G,w}||_\infty = \max_{g \in G} P_{G,w}(g)$. Then we have:

Theorem 4. *Let Γ be a finitely generated linear group. Suppose for some $n \geq 1$ and $1 \neq w \in F_n$ there exists $\epsilon > 0$ such that for all finite quotients G of Γ we have $||P_{G,w}||_\infty \geq \epsilon$. Then Γ is virtually solvable.*

.

2. Proof of Theorem 2

If a group Γ acts on a space X and $Y \subseteq X$, we say Y is Γ-*finite* if its orbit under Γ is finite. We say a closed subset $Z \subseteq X$ is Γ-*covered* by Y if Z is a closed subset of some finite union of Γ-translates of Y.

Lemma 5. *Let Γ be a group acting on a set X. If $Y_1, \ldots, Y_n$ are subsets of X which are not Γ-finite, then there exists $g \in \Gamma$ such that $gY_i \neq Y_j$ for $1 \leq i, j \leq n$.*

Proof. For given i, j, the set of g such that $gY_i = Y_j$ is either empty or is a left coset of the stabilizer of Y_i in Γ. By a theorem of B. H. Neumann [N1], a group cannot be Γ-covered by a finite collection of left cosets of subgroups of infinite index. $\square$

Proposition 6. *Let X be a Noetherian topological space and Γ a group of homeomorphisms $X \to X$. Let f denote a function from the set of closed subsets of X to $[0, 1]$ satisfying the following conditions:*

I. *If $Z \subseteq Y$ are closed subsets of X, then $f(Z) \leq f(Y)$.*
II. *For all closed $Y \subseteq X$ and all $g \in \Gamma$ such that $f(Y \cap gY) = 0$, we have*
$$f(Y \cup gY) \geq 2f(Y).$$

If $Y \subseteq X$ is closed and Γ-covers some closed subset $W \subseteq X$ with $f(W) > 0$, then it Γ-covers some closed Γ-stable subset $Z \subseteq X$ with $f(Z) > 0$.

Proof. By the Noetherian hypothesis, we may assume without loss of generality that Y is minimal for the property of Γ-covering a set of positive f-value. If two distinct irreducible components Y_i and Y_j of Y were Γ-translates of one another, we could replace Y with the union of all of its components except Y_j, and the resulting closed set would still Γ-cover a set of positive f-value. This is impossible by the minimality of Y.

If Y is Γ-finite, then

$$Z := \bigcup_{g \in \Gamma} gY$$

is a Γ-stable finite union of Γ-translates of Y containing W. By condition I, it satisfies $f(Z) > 0$, so we are done. As Y as a finite union of irreducible components, we may therefore assume at least one such component Y_0 is not Γ-finite. We write $Y = Y_0 \cup Y'$, where no Γ-translate of Y' contains Y_0.

By condition I, there exists a finite sequence $g_1, \ldots, g_r \in \Gamma$ such that $f(Z) > 0$ for

$$Z := g_1 Y \cup \cdots \cup g_r Y.$$

We choose the g_i so that

$$(1) \qquad f(Z) > \frac{\sup_{\Delta \subsetneq \Gamma \text{ finite}} f\left(\bigcup_{g \in \Delta} gY\right)}{2}.$$

As no Γ-translate of Y_0 is Γ-finite, Lemma 5 implies there exists g such that $g_i Y_0 \neq g g_j Y_0$ for all i, j. Thus,

$$Y' \cup \bigcup_{i,j} (Y_0 \cap g_i^{-1} g g_j Y_0) \subsetneq Y$$

Γ-covers $Z \cap gZ$. By the minimality of Y, this means $f(Z \cap gZ) = 0$. By condition II, $f(Z \cup gZ) \geq 2f(Z)$, which contradicts (1). We conclude that Z must be Γ-finite.

$\square$

Now, let A be an integral domain finitely generated over $\mathbb{Z}$ with fraction field K. Let $\mathcal{G} = \operatorname{Spec} B$ be an affine group scheme of finite type over A. As usual, for every commutative A-algebra T, $\mathcal{G}(T)$ will denote the set of Spec T-points of $\mathcal{G}$, i.e., the set of A-algebra homomorphisms $B \to T$. The group structure on $\mathcal{G}$ makes each $\mathcal{G}(T)$ a group, functorially in T. We regard $\mathcal{G}$ as a topological space with respect to its Zariski topology. If $Y \subseteq \mathcal{G}$ is a closed subset, we define $Y(T)$ to be the subset of $\mathcal{G}(T)$ consisting of A-homomorphisms $B \to T$ such that

the corresponding map of topological spaces $\mathrm{Spec}\, T \to \mathcal{G}$ sends $\mathrm{Spec}\, T$ into a subset of Y. If $Z \subseteq \mathcal{G}$ is another closed subset, then

$$(Y \cap Z)(T) = Y(T) \cap Z(T),$$

but in general, the inclusion

$$Y(T) \cup Z(T) \subseteq (Y \cup Z)(T)$$

need not be an equality.

We define

$$P(\mathcal{G}, A) := \prod_{\mathfrak{m} \in \mathrm{Maxspec}(A)} \mathcal{G}(A/\mathfrak{m}),$$

where Maxspec denotes the set of maximal ideals, and $P(\mathcal{G}, A)$ is endowed with the product topology. Note that as $\mathcal{G}$ is of finite type (i.e., B is a finitely generated A-algebra) and every $A/\mathfrak{m}$ is a field finitely generated over $\mathbb{Z}$ (and hence finite), it follows that each $\mathcal{G}(A/\mathfrak{m})$ is finite and $P(\mathcal{G}, A)$ is a profinite group. For any closed subset $X \subseteq \mathcal{G}$, we define the closed subset

$$P(X, A) := \prod_{\mathfrak{m} \in \mathrm{Maxspec}(A)} X(A/\mathfrak{m}) \subseteq P(\mathcal{G}, A).$$

Lemma 7. *If $X \subseteq \mathcal{G}$ does not meet the generic fiber $\mathrm{Spec}\, B \otimes_A K \subset \mathcal{G}$, then $P(X, A)$ is empty.*

Proof. If $I \subseteq B$ is the ideal defining X, then $(B/I) \otimes_A K = 0$, so $I \otimes_A K = B \otimes_A K$. It follows that there exist elements $b_i \in I$ and $a_i/a_i' \in K$ such that

$$\sum_i b_i \otimes \frac{a_i}{a_i'} = 1,$$

and clearing denominators, we see that some non-zero element $f := \prod_i a_i' \in A$ belongs to I. If $\mathfrak{m}$ is a maximal ideal of $A[1/f]$, then $A[1/f]/\mathfrak{m}$ is a field finitely generated over $\mathbb{Z}$, hence a finite field, and therefore $\mathfrak{m} \cap A$ is a maximal ideal of A. Thus, the image of f in $A/(\mathfrak{m} \cap A)$ is non-zero, from which it follows that there are no A-homomorphisms $B/I \to A/(\mathfrak{m} \cap A)$, i.e., $X(A/(\mathfrak{m} \cap A)) = \emptyset$. $\qquad\square$

For any subgroup $\Gamma \subseteq \mathcal{G}(A) \subseteq P(\mathcal{G}, A)$, we define $\overline{\Gamma}$ to be the closure of Γ in $P(\mathcal{G}, A)$. This is a closed subgroup of a profinite group and therefore a profinite group itself. We endow it with Haar measure $\mu_{\overline{\Gamma}}$ normalized so that $(\overline{\Gamma}, \mu_{\overline{\Gamma}})$ is a probability space. In particular, left translation by Γ is a continuous measure-preserving action on $(\overline{\Gamma}, \mu_{\overline{\Gamma}})$. As Haar measure is outer regular, for every Borel set B,

$$\mu_{\overline{\Gamma}}(B) = \inf_{S \subseteq \mathrm{Maxspec}(A)} \frac{|\mathrm{pr}_S B|}{|\mathrm{pr}_S \Gamma|},$$

where S ranges over all finite sets of maximal ideals of A and pr_S denotes projection onto $\prod_{\mathfrak{m} \in S} \mathcal{G}(A/\mathfrak{m})$.

For any positive integer n, we let $\mathcal{G}^n$ denote the nth fiber power of $\mathcal{G}$ relative to A, i.e., defining

$$B_n := \underbrace{B \otimes_A B \otimes_A \cdots \otimes_A B}_{n},$$

we define $\mathcal{G}^n := \operatorname{Spec} B_n$, regarded as a topological space with respect to the Zariski topology. Note that in general the Zariski topology on $\mathcal{G}^n$ is *not* the product topology. However, by the universal property of tensor products, $\mathcal{G}^n(T)$ is canonically isomorphic to $\mathcal{G}(T)^n$ for all commutative A-algebras T. Moreover, B_n is a finitely generated $\mathbb{Z}$-algebra, and by the Hilbert basis theorem, this implies that $\mathcal{G}^n$ is a Noetherian topological space.

We consider the closure $\overline{\Gamma}^n$ of Γ^n in $P(\mathcal{G}^n, A)$. For any closed subset $Y \subseteq \mathcal{G}^n$, we define

$$P_\Gamma(Y) := \overline{\Gamma}^n \cap P(Y, A).$$

Thus, if Y and Z are closed subsets of $\mathcal{G}^n$,

$$P_\Gamma(Y \cap Z) = \overline{\Gamma}^n \cap P(Y \cap Z, A) = \overline{\Gamma}^n \cap (P(Y, A) \cap P(Z, A)) = P_\Gamma(Y) \cap P_\Gamma(Z).$$

As

$$P(Y \cup Z, A) = \prod_{\mathfrak{m} \in \operatorname{Maxspec}(A)} (Y(A/\mathfrak{m}) \cup Z(A/\mathfrak{m})) \supseteq P(Y, A) \cup P(Z, A),$$

we have

$$P_\Gamma(Y \cup Z) \supseteq P_\Gamma(Y) \cup P_\Gamma(Z).$$

Defining

$$f(Y) := \mu_{\overline{\Gamma}^n}(P_\Gamma(Y)),$$

condition I of Proposition 6 is obvious. As $\mu_{\overline{\Gamma}^n}$ is a measure, if $f(Y \cap Z) = 0$, then

$$\begin{aligned} f(Y \cup Z) &= \mu_{\overline{\Gamma}^n}(P_\Gamma(Y \cup Z)) \\ &\geq \mu_{\overline{\Gamma}^n}(P_\Gamma(Y) \cup P_\Gamma(Z)) \\ &= \mu_{\overline{\Gamma}^n}(P_\Gamma(Y)) + \mu_{\overline{\Gamma}^n}(P_\Gamma(Z)) - \mu_{\overline{\Gamma}^n}(P_\Gamma(Y) \cap P_\Gamma(Z)) \\ &= f(Y) + f(Z) - f(Y \cap Z) = f(Y) + f(Z). \end{aligned}$$

As $\mu_{\overline{\Gamma}^n}$ is Γ^n-invariant, this implies condition II.

Proposition 8. *Let G denote a linear algebraic group over a field K. If Γ is Zariski dense in $G(K)$, then a non-empty closed subset Y of G^n is Γ^n-finite if and only if it is a union of connected components of G^n.*

Proof. If Y is Γ^n-finite, its stabilizer Δ is of finite index in Γ^n, which implies that the Zariski closure D of Δ in G^n has finite index in G^n. Thus $D \cap (G^n)^\circ$ is of finite index in $(G^n)^\circ$. As $(G^n)^\circ$ is connected, it follows that D contains $(G^n)^\circ$. The Zariski-closure of any left coset of Γ^n is a left coset of D and therefore a union of cosets of $(G^n)^\circ$. Conversely, any left translate of a coset of $(G^n)^\circ$ is again such a coset, so the orbit of any union of connected components of G^n is finite. $\square$

Proposition 9. *Let K be a field and G a reductive algebraic group over K with adjoint semisimple identity component. Let $w \in F_n$ be a non-trivial word and $g_0 \in G(K)$. Then $w^{-1}(g_0)$ does not contain any connected component of G^n.*

Proof. Without loss of generality, we assume K algebraically is closed. Let G° be the identity component, T a maximal torus of G° and B a Borel subgroup of G° containing T. Let Φ be the root system of G with respect to T, and let Φ^+ denote the set of roots of B with respect to T. Every maximal torus of G° is conjugate under $G^\circ(K)$ to T. The Weyl group $N_G(T)/T$ acts transitively on the set of Weyl chambers, so every pair $T' \subset B'$ is conjugate to $T \subset B$ by some element of $G^\circ(K)$. In particular, for any $g \in G(K)$, the pair $g^{-1}Tg \subset g^{-1}Bg$ is conjugate in $G^\circ(K)$ to $T \subset B$, or equivalently, there is some element $h \in gG^\circ(K)$ such that conjugation by h stabilizes T and B. The highest root α of Φ^+ is determined by B, so h likewise preserves α. It therefore normalizes $\ker \alpha^\circ$, and therefore the derived group G_α of the centralizer of $\ker \alpha^\circ$. This group is semisimple and of type A_1, so every element that normalizes it acts by an inner automorphism. It follows that the centralizer of G_α in G meets every connected component of G.

Suppose now that w is constant on $g_1 G^\circ \times \cdots \times g_n G^\circ$ for some $g_1, \ldots, g_n \in G(K)$. Without loss of generality we may assume that all g_i centralize G_α. As w is constant on $g_1 G_\alpha \times \cdots \times g_n G_\alpha$, and as

$$w(g_1 h_1, \ldots, g_n h_n) = w(g_1, \ldots, g_n)w(h_1, \ldots, h_n)$$

for all $h_1, \ldots, h_n \in G_\alpha(K)$, it follows that w is constant on G_α^n. This is impossible because non-trivial words give non-trivial word maps on all semisimple algebraic groups [Bo]. $\square$

We can now prove Theorem 2.

Proof. It is clear that every virtually solvable group satisfies an identity and therefore satisfies a probabilistic identity. For the other direction, we fix a faithful representation $\Gamma \to \mathrm{GL}_k(F)$, where F is a field, which we may assume algebraically closed. Let $H \subset \mathrm{GL}_k$ denote the Zariski

closure of Γ in GL_k. Let G denote the quotient of H by its maximal solvable normal subgroup. As Γ is not virtually solvable, the same is true of G, so H is not finite. Its identity component is therefore a non-trivial adjoint semisimple group.

As G is a linear algebraic group, we can regard it as a closed subgroup of GL_r for some r, so we have a homomorphism $\rho\colon \Gamma \to \mathrm{GL}_r(F)$ such that the Zariski closure of $\rho(\Gamma)$ is G. We recall how to extend G to a subgroup scheme of GL_r defined over a finitely generated $\mathbb{Z}$-algebra. Let

$$R_{\mathbb{Z},r} := \mathbb{Z}[x_{ij}, y]_{i,j=1,\ldots,r}/(y\det(x_{ij}) - 1)$$

denote the coordinate ring of GL_r over $\mathbb{Z}$, and let

$$\Delta_{\mathbb{Z},r}\colon R_{\mathbb{Z},r} \to R_{\mathbb{Z},r} \otimes_{\mathbb{Z}} R_{\mathbb{Z},r},$$

$$S_{\mathbb{Z},r}\colon R_{\mathbb{Z},r} \to R_{\mathbb{Z},r},$$

and

$$\epsilon_{\mathbb{Z},r}\colon R_{\mathbb{Z},r} \to \mathbb{Z}$$

denote the ring homomorphisms associated to the multiplication, inverse, and unit maps. Closed subschemes of GL_r over any commutative ring A are in one-to-one correspondence with ideals I of $R_{A,r} := A \otimes_{\mathbb{Z}} R_{\mathbb{Z},r}$, and such an ideal defines a group subscheme if and only I is a Hopf ideal [Wa, §2.1], i.e., if and only if it satisfies the following three conditions:

$$\Delta_{A,r}(I) \subseteq I \otimes_A R_{A,r} + R_{A,r} \otimes_A I,$$

$$S_{A,r}(I) \subseteq I,$$

$$\epsilon_{A,r}(I) = \{0\}.$$

We fix a finite set of generators h_k of the ideal I_F in $R_{F,r}$ associated to G as a closed subvariety of GL_r over F. We lift each h_k to an element $\tilde{h}_k \in F[x_{ij}, y]$. For any subring $A \subseteq F$ such that $\tilde{h}_k \in A[x_{ij}, y]$, we denote again by h_k the image of $\tilde{h}_k$ in $R_{A,r}$; this should not cause confusion. Let A_0 denote the subring of F generated by all matrix entries in $\mathrm{GL}_r(F)$ of the $\rho(g_j)$, as g_j runs over some finite generating set of Γ, together with all coefficients of the $\tilde{h}_k$. Let I_0 denote the ideal generated by the elements h_k in $R_{A_0,r}$, and let K denote the fraction field of A_0. As

$$\Delta_{A_0,r}(I_0) \subseteq I_0 \otimes_{A_0} R_{K,r} + R_{K,r} \otimes_{A_0} I_0$$

and

$$S_{A_0,r}(I_0) \subseteq I_0 \otimes_{A_0} R_{K,r},$$

there exists $f \in A_0$ such that

$$\Delta_{A_0,r}(h_i) \in I_0 \otimes_{A_0} R_{A_0[1/f],r} + R_{A_0[1/f],r} \otimes_{A_0} I_0$$

and
$$S_{A_0,r}(h_i) \in I_0 \otimes_{A_0} A_0[1/f]$$
for all i, and therefore, setting $A := A_0[1/f]$ and $I := I_0 \otimes_{A_0} A$, we have that I is a Hopf ideal of $R_{A,r}$. We set $\mathcal{G} := \operatorname{Spec} R_{A,r}/I$, the closed group subscheme of GL_r over A defined by $h_k \in R_{A,r}$. By construction, $\rho(\Gamma)$ is a Zariski-dense finitely generated subgroup of $\mathcal{G}(A)$.

Let $Y := w^{-1}(g) \subseteq \mathcal{G}^n$. We define f as above. If $f(Y) > 0$, then Y Γ-covers a set of positive f-value, so by Proposition 6, Y Γ-covers a closed Γ-stable subset Z with $f(Z) > 0$. By Lemma 7, Z must meet the generic fiber G^n of $\mathcal{G}^n$, which implies that Y must meet the generic fiber. Proposition 8 now implies that $Z \cap G^n$ contains a connected component of G^n, and it follows that $Y \cap G^n$ contains a connected component. However, this is impossible by Proposition 9. Thus, $f(Y) = 0$.

Therefore, for every ϵ, there exists a finite set S of maximal ideals of A such that
$$\frac{|\operatorname{pr}_S w^{-1}(g)|}{\operatorname{pr}_S \Gamma^n} < \epsilon.$$
Defining Δ to be the kernel of pr_S, we complete the proof of Theorem 2 (as well as of Theorem 4).

$\square$

3. Open problems

In this section we discuss related open problems concerning finite and residually finite groups.

Problem 10. *Do all finitely generated residually finite groups which satisfy a probabilistic identity satisfy an identity?*

We also pose a related, finitary version of Problem 10.

Problem 11. *Is it true that, for any word $1 \neq w \in F_n$, any positive integer d and any real number $\epsilon > 0$, there exists a word $1 \neq v \in F_m$ (for some m) such that, if G is a finite d-generated group satisfying $P_G(w) \geq \epsilon$, then v is an identity of G?*

Clearly, a positive answer to Problem 11 implies a positive answer to Problem 10. Both seem to be very challenging questions, which might have negative answers in general. However, in some special cases they are solved affirmatively. For example, if $w = [x_1, x_2]$ or $w = x_1^2$, then it is known (see [N2] and [Ma]) that for a finite group G, if $P_G(w) \geq \epsilon > 0$, then G is bounded-by-abelian-by-bounded (in terms of ϵ). This implies

affirmative answers to Problems 10 and 11 for these particular words w.

In general we cannot answer these problems for words of the form x_1^k ($k > 2$). However, for a prime p, a result of Khukhro [Kh] shows that, if G is a finitely generated pro-p group satisfying a coset identity x_1^p (namely there is a coset of an open subgroup consisting of elements of order p or 1) then G is virtually nilpotent (and hence satisfies an identity).

Another positive indication is the result showing that for a (non-abelian) finite simple group T and a non-trivial word w we have $P_T(w) \to 0$ as $|T| \to \infty$ (see [DPPS] for this result, and also [LS] for upper bounds on $P_T(w)$ of the from $|T|^{-\alpha_w}$). This implies that a finite simple group T satisfying $P_T(w) \geq \epsilon > 0$ is of bounded size, hence it satisfies an identity (depending on w and ϵ only).

Affirmative answers to Problems 10 and 11 would have far reaching applications. The argument proving Theorem 1 above also proves the following.

Proposition 12. *Assume Problem 10 has a positive answer, and let Γ be a finitely generated residually finite group. Then either Γ satisfies an identity or Γ is randomly free.*

In particular,

(i) If Γ does not satisfy an identity then $\widehat{\Gamma}$ has a nonabelian free subgroup.

(ii) If $\widehat{\Gamma}$ has a nonabelian free subgroup then almost all n-tuples in $\widehat{\Gamma}$ freely generate a free subgroup.

The next application concerns residual properties of free groups. It is well known that the free group F_n is residually-p. But when is it residually X for a collection X of finite p-groups? If this is the case then F_n is also residually Y where Y is the subset of X consisting of n-generated p-groups. Thus we may replace X by Y and assume all p-groups in X are n-generated. It is also clear that if F_n ($n > 1$) is residually X then the groups in X do not satisfy a common identity (namely they generate the variety of all groups).

It turns out that, assuming an affirmative answer to Problem 11, these conditions are also sufficient.

Proposition 13. *Assume Problem 11 has a positive answer. Let $n \geq 2$ be an integer, p a prime, and X a set of n-generated finite p-groups. Then the free group F_n is residually X if and only if the groups in X do not satisfy a common identity.*

To prove this, suppose the groups in X do not satisfy a common identity. To show that F_n is residually X we have to find, for each $1 \neq w = w(x_1, \ldots, x_n) \in F_n$, a group $G \in X$ and an epimorphism $\phi : F_n \to G$, such that $\phi(w) \neq 1$. This amounts to finding a group $G \in X$ and an n-tuple $g_1, \ldots, g_n \in G$ generating G such that $w(g_1, \ldots, g_n) \neq 1$ (and then ϕ is defined by sending x_i to g_i). Suppose, given w, that there is no $G \in X$ with such an n-tuple. Then, for every $G \in X$, and every generating n-tuple $(g_1, \ldots, g_n) \in G^n$, we have $w(g_1, \ldots, g_n) = 1$. Now, the probability that a random n-tuple in G^n generates G is the probability that its image in V^n spans V, where $V = G/\Phi(G)$ is the Frattini quotient of G, regarded a vector space of dimension $\leq n$ over the field with p elements. This probability is at least $\epsilon := \prod_{i=1}^{n}(1 - p^{-i}) > 0$. Thus $P_G(w) \geq \epsilon$ for all $G \in X$. By the affirmative answer to Problem 11, all the groups $G \in X$ satisfy a common identity $v \neq 1$ (which depends on w, n and p). This contradiction proves Proposition 13.

This argument can be generalized to cases when X consists of finite groups G with the property that n random elements of G generate G with probability bounded away from zero. See [JP] and the references therein for the description of such groups and the related notion of positively finitely generated profinite groups.

References

[Bo]   A. Borel, On free subgroups of semisimple groups, *Enseign. Math.* **29** (1983), 151–164.

[BG]   E. Breuillard and T. Gelander, A topological Tits alternative, *Annals of Math.* **166** (2007), 427–474.

[DPPS] J.D. Dixon, L. Pyber, Á. Seress, A. Shalev, Residual properties of free groups and probabilistic methods, *J. reine angew. Math. (Crelle's)* **556** (2003), 159–172.

[Ep]   D.B.A. Epstein, Almost all subgroups of a Lie group are free, *J. Algebra* **19** (1971), 261-262.

[JP]   A. Jaikin-Zapirain and L. Pyber, Random generation of finite groups and profinite groups and group enumeration, *Annals of Math.* **173** (2011), 769–814.

[Kh]   E.I. Khukhro, Locally nilpotent groups that admit a splitting automorphism of prime order, *Mat. Sb.* (N.S.) **130(172)** (1986), 120-127, 128.

[LS]   M. Larsen and A. Shalev, Fibers of word maps and some applications, *J. Algebra* **354** (2012), 36–48.

[Ma]   A. Mann, Finite groups containing many involutions, *Proc. Amer. Math. Soc.* **122** (1994), 383–385.

[N1]   B.H. Neumann, Groups covered by finitely many cosets, *Publ. Math. Debrecen* **3** (1954), 227–242.

[N2]   P.M. Neumann, Two combinatorial problems in group theory, *Bull. London Math. Soc.* **21** (1989), 456–458.
[Ti]   J. Tits, Free subgroups in linear groups, *J. Algebra* **20** (1972), 250–270.
[Wa]   W.C. Waterhouse, Introduction to affine group schemes. Graduate Texts in Mathematics, 66. Springer-Verlag, New York-Berlin, 1979.

E-mail address: mjlarsen@indiana.edu

DEPARTMENT OF MATHEMATICS, INDIANA UNIVERSITY, BLOOMINGTON, IN 47405, U.S.A.

E-mail address: shalev@math.huji.ac.il

EINSTEIN INSTITUTE OF MATHEMATICS, HEBREW UNIVERSITY, GIVAT RAM, JERUSALEM 91904, ISRAEL